CLAIMS

1.   A method for producing ephemeral encryption keys at a first station for use in a communication session with a second station, comprising:

assigning an ephemeral session key in said first station, in response to a request received by said first station during a session random key initiation interval for use in a first exchange of said plurality of exchanges;

associating, in said first station, a set of ephemeral intermediate data random keys with said request for use in said plurality of exchanges;

sending at least one message carrying said session key to the second station, and receiving a response from the second station including a shared parameter, which is shared between the first station and the second station, or between the first station and a user at the second station, encrypted using said session random key verifying receipt of the session random key; and

sending, after verifying receipt of the session random key at the second station, at least one message carrying an encrypted version of one of said set of ephemeral intermediate data random keys encrypted to be accepted as an encryption key for the session.

2.   The method of claim 1, including assigning said session random key to all communication sessions initiated with the first station, during said session random key initiation interval.

3.   The method of claim 1, including assigning said session random key to all communication sessions initiated with the first station during said session random key initiation interval, and associating a different set of ephemeral intermediate data random keys with each communication session.

4.   The method of claim 1, including
providing a buffer at the first station;
storing said ephemeral session random keys in the buffer;
associating respective session random key initiation intervals with said ephemeral

5 session random keys stored in said buffer;

6 using ephemeral session random keys from said buffer as session random keys in

7 response to requests received by said first station during said respective session random

8 key initiation intervals;

9 removing ephemeral session random keys from said buffer after expiry of the

10 respective session random key lifetime in the buffer.

1 5. The method of claim 4, wherein said buffer is managed as a circular buffer.

1 6. The method of claim 4, wherein a session random key lifetime in the buffer for

2 said plurality of exchanges has a value within which the plurality of exchanges can be

3 completed in expected circumstances, and said ephemeral session random keys are

4 removed from said buffer after a multiple M times said value of session random key

5 lifetime to engage into establishing a communication session, where M is less than or

6 equal to 10.

1 7. The method of claim 4, wherein a session random key lifetime in the buffer for

2 said plurality of exchanges has a value within which the plurality of exchanges can be

3 completed in expected circumstances, and said ephemeral session random keys are

4 removed from said buffer after a multiple M times said value, and the session random

5 key lifetime to engage into establishing a communication session is less than about 90

6 seconds.

1 8. A data processing apparatus, comprising:

2 a processor, a communication interface adapted for connection to a

3 communication medium, and memory storing instructions for execution by the data

4 processor, the instructions including

5 logic to receive a request via the communication interface for initiation of a

6 communication session between a first station and a second station;

7 logic to provide ephemeral encryption keys at the first station, in response to a

8 request received by said first station during a session random key initiation interval for

9 use in a first exchange of said plurality of exchanges, to associate, in said first station, a

10 set of ephemeral intermediate data random keys with said request for use in said plurality

11 of exchanges, and logic to send at least one message carrying said session random key to

12 the second station, and to receive a response from the second station including a shared

13 parameter encrypted using said session random key verifying receipt of the session

14 random key; and

15 logic to send, after verifying receipt of the session random key at the second

16 station, at least one message carrying an encrypted version of one of said set of

17 ephemeral intermediate data random keys encrypted to be accepted as an encryption key

18 for the session.

1 9. The apparatus of claim 8, including logic to assign said session random key to all

2 communication sessions initiated with the first station, during said session random key

3 initiation interval.

1 10. The apparatus of claim 8, including logic to assign said session random key to all

2 communication sessions initiated with the first station during said session random key

3 initiation interval, and to associate a different set of ephemeral intermediate data random

4 keys with each communication session.

1 11. The apparatus of claim 8, including

2 a buffer at the first station;

3 logic to store said ephemeral session random keys in the buffer, to associate

4 respective session random key initiation intervals with said ephemeral session random

5 keys stored in said buffer, to use ephemeral session random keys from said buffer as

6 session random keys in response to requests received by said first station during said

7 respective session random key initiation intervals, and to remove ephemeral session

8 random keys from said buffer after expiry of the respective session random key lifetime

9 in the buffer.

1 12. The apparatus of claim 11, wherein said buffer comprises a circular buffer.

1 13. The apparatus of claim 11, wherein a session random key lifetime in the buffer for
2 said plurality of exchanges has a value within which the plurality of exchanges can be
3 completed in expected circumstances, and logic to remove said ephemeral session
4 random keys from said buffer after a multiple M times said value of session random key
5 lifetime to engage into establishing a communication session, where M is less than or
6 equal to 10.

1 14. The apparatus of claim 11, wherein a predicted lifetime for said plurality of
2 exchanges has a value within which the plurality of exchanges can be completed in
3 expected circumstances, and logic to remove said ephemeral session random keys from
4 said buffer after a multiple M times said value, and the session random key lifetime to
5 engage into establishing a communication session is less than about 90 seconds.

1 15. An article, comprising:
2 machine readable data storage medium having computer program instructions stored
3 therein for establishing a communication session on a communication medium between a
4 first data processing station and a second data processing station having access to the
5 communication medium, said instructions comprising
6   logic to receive a request via the communication interface for initiation of a
7 communication session between a first station and a second station;
8   logic to provide ephemeral encryption keys at the first station, in response to a
9 request received by said first station during a session random key initiation interval for
10 use in a first exchange of said plurality of exchanges, to associate, in said first station, a
11 set of ephemeral intermediate data random keys with said request for use in said plurality
12 of exchanges, and logic to send at least one message carrying said session random key to
13 the second station, and to receive a response from the second station including a shared
14 parameter encrypted using said session random key verifying receipt of the session
15 random key; and
16   logic to send, after verifying receipt of the session random key at the second
17 station, at least one message carrying an encrypted version of one of said set of

18   ephemeral intermediate data random keys encrypted to be accepted as an encryption key

19   for the session.

1   16.   The article of claim 15, wherein the instructions include logic to assign said

2   session random key to all communication sessions initiated with the first station, during

3   said session random key initiation interval.

1   17.   The article of claim 15, wherein the instructions include logic to assign said

2   session random key to all communication sessions initiated with the first station during

3   said session random key initiation interval, and to associate a different set of ephemeral

4   intermediate data random keys with each communication session.

1   18.   The article of claim 15, including

2   a buffer at the first station; and

3   the instructions include logic to store said ephemeral session random keys in the

4   buffer, to associate respective session random key initiation intervals with said ephemeral

5   session random keys stored in said buffer, to use ephemeral session random keys from

6   said buffer as session random keys in response to requests received by said first station

7   during said respective session random key initiation intervals, and to remove ephemeral

8   session random keys from said buffer after expiry of the respective session random key

9   lifetime in the buffer.

1   19.   The article of claim 18, wherein said buffer comprises a circular buffer.

1   20.   The article of claim 18, wherein a session random key lifetime in the buffer for

2   said plurality of exchanges has a value within which the plurality of exchanges can be

3   completed in expected circumstances, and the instructions include logic to remove said

4   ephemeral session random keys from said buffer after a multiple M times said value of

5   session random key lifetime to engage into establishing a communication session, where

6   M is less than or equal to 10.

1 21.   The article of claim 18, wherein a session random key lifetime in the buffer for

2 said plurality of exchanges has a value within which the plurality of exchanges can be

3 completed in expected circumstances, and the instructions include logic to remove said

4 ephemeral session random keys from said buffer after a multiple M times said value, and

5 the session random key lifetime to engage into establishing a communication session is

6 less than about 90 seconds.